EXHIBIT B

(UNDER SEAL)

I attest and certify on 11-15-17 that this is a full true and correct copy of the original document.

PEGGY A. LEEN
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA

By J. Hoskin ___Deputy ✓Secretary

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Nevada

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2216 TONA CIRCLE, LAS VEGAS, NEVADA 89169. A-2

Case No. 2:17-mj-1084-PAL

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Nevada
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENTS B and C

✓ **YOU ARE COMMANDED** to execute this warrant on or before November 29, 2017 *(not to exceed 14 days)*
✓ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to PEGGY A. LEEN
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 11-15-17 9:02 am

Peggy A. Leen
Judge's signature

City and state: Las Vegas, Nevada

PEGGY A. LEEN
U.S. MAGISTRATE JUDGE
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:17-mj-	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT C

Protocol For Searching The Electronic Data Seized Pursuant To This Search Warrant

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond

those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

> (e) Issuing the Warrant.
> (2) Contents of the Warrant.
> (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:
> (i) execute the warrant within a specified time no longer than 14 days;
> (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.
> (f) Executing and Returning the Warrant.
> (1) Warrant to Search for and Seize a Person or Property.
> (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, but no later than any return deadline specified in the warrant, if earlier, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian, in the case of data held by a third-party service provider, or when the United States begins copying a complete forensic image of the target electronic device, in the case of data contained within an electronic device; in either case, execution of this warrant is complete when the United States obtains a complete copy of the Search Warrant Data. Within fourteen (14) days of completion of the execution of the warrant, but no later than any return deadline specified in the warrant, if earlier, the inventory will be filed with the Court.

b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search

Warrant Data be retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

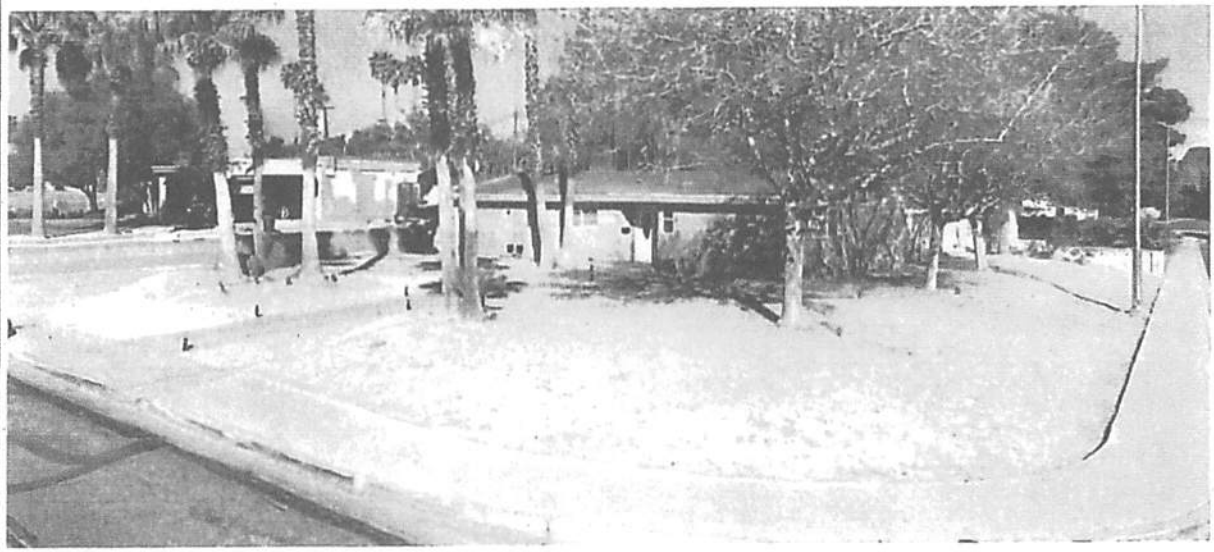
SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

ATTACHMENT A-2

Property to Be Searched

The **TARGET PREMISES** include the residence located at **2216 TONA CIRCLE**, as well as any vehicles, outbuildings, storage lockers (including safes), and electronic media (e.g., computers, wireless telephones, and other storage media, such as scanners, external storage media, and printers with memory capability) located thereon. As depicted in the image below, the residence is located closest to the major cross streets of Desert Inn and Eastern in Las Vegas, NV. The residence is located in the northern most part of a cul-de-sac on the west side of the block. The numbers "2216" are firmly affixed in black numbers to the south of the front door. They also appear, in paint, on the front curb with black numbers and a white background. The residence is gray in color and appears to be either stripped of paint for potential painting or in disrepair. The residence has a red shingle roof. The front door is yellow and faces east.



ATTACHMENT B

1. All records and information from October 1, 2011 to present that constitute fruits, contraband, evidence, and instrumentalities of violations of 17 U.S.C. § 506 and 18 U.S.C. § 2319 (Criminal Copyright Infringement), 18 U.S.C. § 371 (Conspiracy), and 18 U.S.C. § 2 (Aiding and Abetting), including:

a. Records and information relating to the reproduction, distribution, public performance, and public display of copyrighted TV shows, movies, and other works without the permission of the copyright owners;

b. Records and information relating to the ownership and operation of Jetflicks and use of the domains jetflicks.mobi, jetflicks.net, jetflicks.com, and sincitygeeks.com, including but not limited to bank statements, other financial statements, receipts and payments for goods and services, inventory lists, payments to employees or contractors, use of advertising, customer lists, email lists, and website traffic data and analytics;

c. Records and information relating to the ownership and operation of iStreamitAll and the use of the domains istreamitall.com and istreamitall.mobi, including but not limited to bank statements, other financial statements, receipts and payments for goods and services, inventory lists, payments to employees or contractors, use of advertising, customer lists, email lists, and website traffic data and analytics;

d. Records and information relating to the operation of Jetflicks and iStreamItAll on streaming platforms including but not limited to personal computers, tablets, Android-based smartphones, Apple iPhones, Roku devices, Amazon Fire TVs, Google Chromecast, Apple TVs or other Airplay devices, Xbox consoles, PlayStation consoles, Wii

consoles, smart TVs, and the development and use of apps, add-ons, channels, and other means in such operation;

e. Records and information relating to the use of programs such as SickRage and Sick Beard to search, locate, download, process, and store copyrighted TV shows, movies, and other works without the permission of the copyright owners;

f. Records and information relating to the use of BitTorrent sites and other peer-to-peer file-sharing sites as well as Usenet sites to search, locate, download, process, and store copyrighted TV shows, movies, and other works without the permission of the copyright owners;

g. Records and information relating to the ownership and operation of SmackDownOnYou, BoxBusters.TV, and Mixtape UG, and the use of the domains smackdownonyou.com, boxbusters.tv, mixtapeug.com;

h. Records and information relating to the identity and location of individuals working for or with Kristopher Dallmann on the operation of Jetflicks including but not limited to Jared Edwards, Grant Dunmire, Darryl Polo, Yoany Vaillant Fajardo, and Luis Villarino;

i. Records and information relating to the identity and location of individuals working for or with Darryl Polo on the operation of iStreamItAll;

j. Records and information relating to notices, letters, emails, and complaints about copyright infringement, piracy, and use of copyrighted works without permission and compensation to the copyright owners;

k. Records and information pertaining to the ownership, control, maintenance, or improvements of the **TARGET PREMISES**, including, but not limited to, utility and telephone bills, rental purchase or lease agreements, keys, and photographs;

l. All containers in which the items described above may be stored, including, but not limited to briefcases, backpacks, bags, shoe boxes, hampers, laundry baskets, safes, storage containers, storage units, lockers, foot lockers, tool boxes, and outbuildings/storage sheds;

m. Records relating to the contracts, keys, codes, or combinations for any briefcases, safes, safety deposit boxes, storage containers, storage units, lockers, foot lockers, tool boxes, or outbuildings/storage sheds in which the items described above may be stored; and

n. any other items, which can be readily identified as connected to the aforementioned crimes or which are subject to seizure pursuant to the laws of the United States of America.

2. Computers or storage medium that may have been used as a means to commit the violations described above;

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer, wireless telephone, or other storage medium that contains or in which are stored records or information that is otherwise called for by this warrant:

a. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Evidence of software that would allow others to control the computer, wireless telephone, or other storage medium, such as viruses, Trojan horses, and other forms of malicious software;

c. Evidence of security software designed to detect the types of malicious software described above;

d. Evidence of the lack of the types of malicious software described above, as well as evidence of the absence of security software designed to detect the types of malicious software described above;

e. Evidence indicating how and when the computer, wireless telephone, or storage medium was accessed or used to determine the chronological context of device access and use and events relating to the crimes under investigation;

f. Evidence indicating the computer, wireless telephone, or other storage medium user's state of mind as it relates to the crimes under investigation;

g. Evidence of the attachment to a computer of a wireless telephone or other storage devices, or similar containers for electronic evidence, or of a wireless telephone or storage medium to other computers or electronic devices;

h. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer, wireless telephone, or other storage medium;

i. Evidence of the times the computer, wireless telephone, or other storage medium was used;

j. Passwords, encryption keys, and other access devices that may be necessary to access the computer, wireless telephone, or other storage medium;

k. Documentation and manuals that may be necessary to access the computer, wireless telephone, or other storage medium or to conduct a forensic examination of the computer, wireless telephone, or other storage medium;

l. Records of or information about Internet Protocol addresses used by the computer, wireless telephone, or other storage medium;

m. Records of, or information about, the computer's, wireless telephone's, or other storage medium's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses; and

n. Contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers, wireless telephones, or other storage medium to the internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.